

(19) Organisation Mondiale de la Propriété
Intellectuelle
Bureau international



(43) Date de la publication internationale
10 janvier 2002 (10.01.2002)

PCT

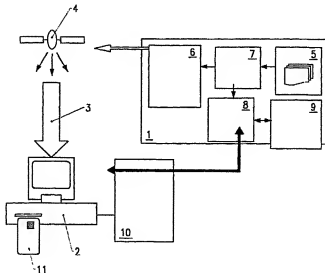
(10) Numéro de publication internationale
WO 02/03694 A1

- (51) Classification internationale des brevets⁷ : H04N 7/16, 7/167, 7/173
- (21) Numéro de la demande internationale : PCT/FR01/02174
- (22) Date de dépôt international : 6 juillet 2001 (06.07.2001)
- (25) Langue de dépôt : français
- (26) Langue de publication : français
- (30) Données relatives à la priorité : 00/08838 6 juillet 2000 (06.07.2000) FR
- (71) Déposant (pour tous les États désignés sauf US) : AT-SKY (SAS) (FR/FR); Voie Atlas, Z.I. Athelia III, F-13600 La Ciotat (FR).
- (72) Inventeurs; et
(75) Inventeurs/Déposants (pour US seulement) : LEROUX, Jean-Yves (FR/FR); 1281 Chemin des Côtes, F-13600 Ceyreste (FR). JABIOL, Laurent (FR/FR); 31, avenue Eugène Julien, F-13600 Ceyreste (FR).
- (74) Mandataire : ROMAN, Michel; 35, rue Paradis, B.P. 2224, F-13207 Marseille Cedex 01 (FR).
- (81) État désigné (national) : US.
- (84) États désignés (régional) : brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).
- Publiée :
— avec rapport de recherche internationale

[Suite sur la page suivante]

(54) Title: SYSTEM FOR CONTROLLING ONLINE AND OFFLINE ACCESS TO DIGITAL DATA USING A SOFTWARE KEY SERVER

(54) Titre : SYSTEME DE CONTRÔLE D'ACCÈS AUX DONNÉES NUMÉRIQUES EN LIGNE ET HORS LIGNE AU MOYEN D'UN SERVEUR DE CLES LOGICIELLES



(57) Abstract: The invention concerns a system for controlling online and offline access to digital data using a software key server. It consists in controlling access to encrypted digital data or programmes broadcast by satellite, cable or digital land-based network, using a server of decryption keys (8) whereby each reception terminal (2) must be connected with a single identification through a secure channel independent of the transmission channel to be able to use the transmitted data or programmes. Said system is generally applicable to all types of digital data transmission, and in particular digital television programmes or encrypted data broadcasting services.

[Suite sur la page suivante]



En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(57) Abrégé : La présente invention a pour objet un système de contrôle d'accès aux données numériques en ligne ou hors ligne au moyen d'un serveur de clés logicielles. Il consiste à contrôler l'accès aux données ou programmes numériques cryptés diffusés par satellite, par câble ou par réseau terrestre numérique, au moyen d'un serveur de clés (8) de décryptage auquel chaque terminal de réception (2) doit se connecter avec une identification unique au travers d'un canal sécurisé indépendant de la voie de transmission pour pouvoir utiliser les données ou programmes transmis. Ce système se rapporte d'une manière générale au domaine de la transmission sous forme numérique d'informations de tous types, et en particulier d'émissions de télévision numérique ou de services de diffusion de données cryptées.

**SYSTÈME DE CONTRÔLE D'ACCÈS AUX DONNÉES NUMÉRIQUES
EN LIGNE ET HORS LIGNE
AU MOYEN D'UN SERVEUR DE CLÉS LOGICIELLES**

5

La présente invention a pour objet un système de contrôle d'accès aux données numériques en ligne ou hors ligne au moyen d'un serveur de clés logicielles.

10

Il se rapporte d'une manière générale au domaine de la transmission sous forme numérique d'informations de tous types, et en particulier d'émissions de télévision numérique ou de services de diffusion de données cryptées.

15

Aujourd'hui, les contrôles d'accès sont utilisés pour protéger l'accès aux bouquets de télévision numériques. Chaque programme crypté peut être déchiffré au moyen d'une carte à puce ayant les droits de déchiffrement et générant les clés de décryptage adéquates à l'aide de clés numériques reçues via les terminaux de réception numérique.

20

Dans certains cas, comme l'achat de programmes (généralement des films), une voie de retour telle qu'un réseau téléphonique est utilisée pour effectuer la facturation ou la décrémentation de jetons pré-payés, puis l'attribution de droits temporaires à la carte à puce, permettant à l'utilisateur de regarder le programme ou le film choisi.

25

Cependant, une fois les droits acquis, le déchiffrement se fait sans connexion grâce aux clés récupérées dans le flux émis qui contient également les services ou programmes cryptés. Ainsi, le fournisseur de services n'a pas de moyen de connaître la liste des utilisateurs (ou cartes à puces) qui déchiffront ses programmes à chaque instant, et de ce fait, n'a aucun moyen de savoir si une carte pirate est utilisée à un moment déterminé.

30

Le système selon la présente invention a pour objectif de remédier à cet état de choses. Il permet en effet à tout fournisseur de services tels que télévision numérique ou informations cryptées de connaître à tout moment, et donc de contrôler efficacement, le groupe d'utilisateurs de ses services.

- Le système permet au fournisseur d'identifier l'ensemble des utilisateurs à chaque instant. Toute carte à puce ou système pirate peut être instantanément identifié grâce à l'unicité de chaque session ouverte, condition obligatoire pour la récupération des clés. Le procédé offre une solution plus
- 5 difficilement "piratable" que l'ensemble des systèmes actuels.

- Le système consiste à contrôler l'accès aux données ou programmes numériques cryptés diffusés par satellite, par câble ou par réseau terrestre numérique, au moyen d'un serveur de clés de décryptage auquel chaque terminal
- 10 de réception doit se connecter avec une identification unique au travers d'un canal sécurisé indépendant de la voie de transmission pour pouvoir utiliser les données ou programmes transmis.

- Sur le dessin annexé, donné à titre d'exemple non limitatif d'une des
- 15 formes de réalisation de l'objet de l'invention, la figure 1 est un schéma synoptique d'un ensemble permettant l'application du système proposé.

- L'ensemble selon la figure 1 est constituée d'une station de diffusion 1 et de terminaux 2 récepteurs d'émissions numériques 3 cryptées transmises par
- 20 exemple par un satellite 4. Les données 5 à émettre par la station 1 du fournisseur sont envoyées vers le réseau satellite grâce à un serveur de données cryptées 6 après passage par un module de cryptage 7.

- La station 1 comporte en outre un module serveur de clés 8 connecté à un contrôleur d'autorisations 9 et relié au réseau téléphonique 10.
- 25 Un lecteur de carte à puce 11 est intégré au terminal 2 de réception ou raccordé à ce dernier.

- Les séances de communication, ou "sessions" sont ouvertes avec le serveur de clés 8 qui identifie les numéros de téléphone et de carte à puce 11
- 30 caractérisant l'utilisateur et ou l'adresse Internet du récepteur 2. Le contrôleur d'autorisations 9 décide ou pas de fournir les clés de décryptage durant toute la session en fonction des droits de l'utilisateur.

Le système décrit peut présenter l'inconvénient d'occuper une ligne téléphonique de façon prolongée entraînant un coût de communication élevé et une gêne occasionnée aux utilisateurs n'ayant qu'une ligne téléphonique.

- 5 Une solution intermédiaire consiste à télécharger plusieurs clés à chaque connexion dans une zone sécurisée (par exemple dans la carte à puce 11 elle même) de façon à libérer la ligne durant l'utilisation de ces clés. A titre indicatif, une connexion de quelques secondes par heure pourrait être suffisante pour charger les clés nécessaires pendant cette période.

- 10 De plus, d'autres moyens de connexion à des serveurs apparaissent, tels les nouveaux systèmes de codage téléphonique (ADSL ou VDSL), le câble, ou la diffusion terrestre numérique, ainsi que les protocoles pour téléphones mobiles (GSM, GPRS, WAP,...) permettant de ne pas monopoliser un accès comme la ligne téléphonique classique.

- 15 Le système peut permettre à des utilisateurs non abonnés d'utiliser "à la carte" un ensemble de services payants. Par exemple, il peut être possible de s'abonner une heure, un jour, une semaine à tel ou tel service. Le coût pouvant être supérieur à un abonnement classique mais laissant libre l'utilisateur. Eventuellement, l'association avec le paiement par carte bancaire peut être envisagé. Ainsi, chaque
20 opérateur a le choix de s'ouvrir à tout utilisateur sans que ce dernier s'engage sur une période de temps prédéfinie, ceci de façon totalement contrôlée, chaque transaction identifiant formellement l'utilisateur de façon unique.

- Des bornes publiques ou récepteurs multi-utilisateurs peuvent
25 permettre à chacun, contrairement aux décodeurs placés chez les particuliers, l'accès à des données et services payants. Chaque utilisateur est muni d'une carte d'accès (carte à puce par exemple, pouvant servir également de carte de paiement), ou d'un code d'accès et d'un mot de passe, ou encore un contrôle biométrique, lui permettant d'accéder aux services souhaités de façon ponctuelle, par exemple dans
30 un hôtel ou un grand magasin. Chaque connexion permet de gérer et contrôler pour chacun un compte distant donnant plus de liberté et de service aux utilisateurs et plus d'offre, contrôlée et sécurisée aux fournisseurs de services.

Le système selon l'invention peut être utilisé dans le domaine des logiciels payants (contrats, licences) ou de la location de matériel.

Aujourd'hui, la protection de l'utilisation frauduleuse de logiciels est généralement faite à l'aide de clés software (numéro de séries) ou hardware (clés appelées "dongles").

Appliqué à ce domaine, le système rend l'utilisation de tout logiciel ou matériel connectable totalement contrôlée par les fournisseurs. Il peut être par exemple appliqué à l'utilisation de :

- logiciels payés à l'heure ou à la journée, les clés envoyées en ligne permettant de maintenir actif le logiciel ou un de ses modules. Par exemple, une partie du logiciel disparaît lorsque les clés ne sont pas reçues rendant ce dernier non opérationnel,
- stations de travail onéreuses, grosses machines industrielles, ce qui permet d'éviter à certaines entreprises d'avoir à les acheter, tout en contrôlant leur utilisation, voire le lieu d'utilisation grâce au numéro de téléphone utilisé,
- ordinateurs individuels placés "gratuitement" directement chez des utilisateurs, ou dans des endroits publics.

Le principe peut aussi s'appliquer au contrôle d'utilisation de matériel ou de logiciel hors-ligne :

L'utilisateur peut soit acheter des cartes pré créditées, soit charger une carte à l'aide d'une connexion en ligne. Cette carte peut permettre l'utilisation ultérieure d'un logiciel ou de matériel sans connexion.

Par exemple, un ordinateur individuel placé gratuitement chez l'utilisateur ne peut fonctionner que si la carte appropriée possède un crédit suffisant.

Cette application peut aussi être associée à un contrôle par flux non connecté : pour pouvoir utiliser le matériel ou le logiciel, non seulement l'utilisateur doit posséder un crédit suffisant, mais pendant le temps de l'utilisation ou une partie, il reçoit des données par une voie descendante sans voie de retour nécessaire (réception satellite par exemple) qui déverrouille l'utilisation du matériel ou logiciel.

La carte créditée peut donner à un système de réception les paramètres nécessaires au filtrage des données de déverrouillage. Par analogie aux systèmes de déverrouillage nécessitant un code d'accès ou un mot de passe, le crédit de l'utilisateur donne au système la possibilité et les paramètres nécessaires

à la réception des codes d'accès ou des mots de passe émis par un système distant permettant l'utilisation désirée.

Le système selon l'invention peut également donner lieu à des applications dans le domaine des outils de réception totalement portable tels que
5 téléphone mobile évolué (réception UTMS, écran d'affichage matriciel évolué), ou «décodeur-téléviseur» mobile, équipés d'un récepteur de flux diffusés et éventuellement de voie de retour mono ou bi-directionnelle sans fil.

10 Le positionnement des divers éléments constitutifs donne à l'objet de l'invention un maximum d'effets utiles qui n'avaient pas été, à ce jour, obtenus par des systèmes similaires.

REVENDECATIONS

- 5 1 . Système de contrôle d'accès aux données numériques en ligne et hors ligne au moyen d'un serveur de clés logicielles, destiné à la transmission de données ou programmes numériques cryptés diffusés par satellite, par câble ou par réseau terrestre numérique,
- caractérisé en ce que le contrôle d'accès aux émissions numériques
- 10 (3) issues d'une station de diffusion (1) est effectué au moyen d'un serveur de clés (8) de décryptage auquel chaque terminal de réception (2) doit se connecter avec une identification unique au travers d'un canal sécurisé indépendant de la voie de transmission des données ou programmes, pour pouvoir utiliser lesdites données ou programmes transmis.
- 15 2 . Système de contrôle d'accès selon la revendication 1, se caractérisant par le fait que la station de diffusion (1) est associée à un module serveur de clés (8) connecté à un contrôleur d'autorisations (9).
- 20 3 . Système de contrôle d'accès selon la revendication 1, se caractérisant par le fait que le module serveur de clés (8) est relié au terminal de réception (2) par un réseau téléphonique (10).
- 4 . Système de contrôle d'accès selon la revendication 3, se
- 25 caractérisant par le fait que plusieurs clés de décryptage sont téléchargées à chaque connexion dans une zone sécurisée telle qu'une carte à puce (11), de façon à pouvoir libérer la ligne durant l'utilisation de ces clés.
- 5 . Système de contrôle d'accès selon l'une quelconque des
- 30 revendications précédentes, se caractérisant par le fait qu'il est agencé pour permettre à des utilisateurs non abonnés d'utiliser à la demande, de façon totalement contrôlée, un ensemble de services payants, chaque transaction identifiant formellement l'utilisateur de façon unique.

6 . Système de contrôle d'accès selon l'une quelconque des revendications précédentes, se caractérisant par le fait que le terminal de réception (2) est relié à un lecteur de carte à puce (11), ladite carte à puce permettant d'identifier l'utilisateur.

5

7 . Système de contrôle d'accès selon l'une quelconque des revendications précédentes, se caractérisant par le fait qu'il est agencé pour permettre l'utilisation de logiciels payants, les clés envoyées en ligne permettant de maintenir actif le logiciel ou un de ses modules.

10

8 . Système de contrôle d'accès selon l'une quelconque des revendications 1 à 6, se caractérisant par le fait qu'il est agencé pour permettre le contrôle de l'utilisation de matériel connectable.

15

9 . Système de contrôle d'accès selon l'une quelconque des revendications 6 à 8, se caractérisant par le fait qu'il permet de contrôler l'utilisation de logiciels ou de matériel hors ligne grâce à une carte de crédit (11) chargée à l'aide d'une connexion en ligne.

20

10 . Système de contrôle d'accès selon la revendication 9, se caractérisant par le fait qu'il permet le contrôle par flux non connecté, l'utilisateur recevant pendant le temps de l'utilisation ou une partie de ce temps des données par une voie descendante sans voie de retour nécessaire (réception satellite par exemple) qui déverrouille l'utilisation du matériel ou logiciel.

25

11 . Système de contrôle d'accès selon l'une quelconque des revendications précédentes, se caractérisant par le fait que le terminal de réception (2) est de type multi-utilisateurs permettant à chacun l'accès à des données et services payants, chaque utilisateur étant muni d'une carte d'accès telle que carte à puce (11) ou d'un code d'accès et d'un mot de passe, ou encore subissant un contrôle biométrique, lui permettant d'accéder aux services souhaités de façon ponctuelle.

30

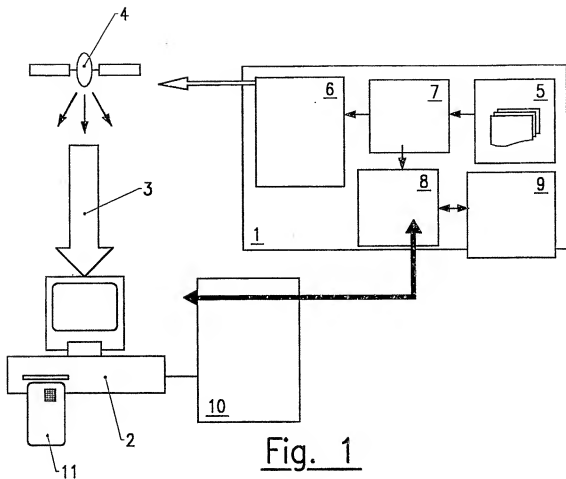
12 . Système de contrôle d'accès selon la revendication 11, se caractérisant par le fait que chaque connexion permet de gérer et contrôler pour chaque utilisateur un compte distant.

5 13. Système de contrôle d'accès selon l'une quelconque des revendications 11 et 12, se caractérisant par le fait qu'il permet de contrôler l'utilisation de logiciels ou de matériel hors ligne grâce à une carte de crédit (11) chargée à l'aide d'une connexion en ligne.

10 14. Système de contrôle d'accès selon l'une quelconque des revendications 1 et 2, se caractérisant par le fait qu'il est adapté pour s'appliquer à des appareils portables tels que téléphone mobile évolué (réception UTMS, écran d'affichage matriciel évolué), ou décodeur-téléviseur mobile, équipés d'un récepteur de flux diffusés.

15 15 . Système de contrôle d'accès selon la revendication 12, se caractérisant par le fait que les appareils portables sont équipés de voie de retour mono ou bi-directionnelle sans fil.

1/1



INTERNATIONAL SEARCH REPORT

 Int. Application No.
 PC17/R 01/02174

A. CLASSIFICATION OF SUBJECT MATTER IPC 7 H04N7/16 H04N7/167 H04N7/173		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) IPC 7 H04N		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the International search (name of data base and, where practical, search terms used) EPO-Internal		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 99 19822 A (MICROSOFT CORP) 22 April 1999 (1999-04-22)	1-3, 7, 8, 15
Y	page 5, line 22 -page 19, line 14 figures 1-7	4-6, 9-13
Y	"FUNCTIONAL MODEL OF A CONDITIONAL ACCESS SYSTEM" EBU REVIEW- TECHNICAL, BE, EUROPEAN BROADCASTING UNION, no. 266, 21 December 1995 (1995-12-21), pages 64-77, XP000559450 Grand Saconnex, CH ISSN: 0251-0936 page 67, right-hand column, line 25 -page 76, right-hand column, line 5 figures 4-7	4-6, 9-13
<input type="checkbox"/> Further documents are listed in the continuation of box C. <input checked="" type="checkbox"/> Patent family members are listed in annex.		
* Special categories of cited documents : *A* document defining the general state of the art which is not considered to be of particular relevance *E* earlier document but published on or after the international filing date *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (see specification) *O* document referring to an oral disclosure, use, exhibition or other means *P* document published prior to the international filing date but later than the priority date claimed *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art *Z* document member of the same patent family		
Date of the actual completion of the international search 18 October 2001		Date of mailing of the international search report 25/10/2001
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3010		Authorized officer Van der Zaai, R

INTERNATIONAL SEARCH REPORT

International Application No.

PCT/JP 01/02174

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9919822 A	22-04-1999	EP 1031206 A2 WO 9919822 A2	30-08-2000 22-04-1999

A. CLASSEMENT DE L'OBJET DE LA DEMANDE CIB 7 H04N7/16 H04N7/167 H04N7/173		
Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB		
B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE Documentation minimale consultée (système de classification suivi des symboles de classement) CIB 7 H04N		
Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche		
Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés) EPO-Internal		
C. DOCUMENTS CONSIDERES COMME PERTINENTS		
Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	W0 99 19822 A (MICROSOFT CORP) 22 avril 1999 (1999-04-22)	1-3, 7, 8, 15
Y	page 5, ligne 22 -page 19, ligne 14 figures 1-7	4-6, 9-13
Y	"FUNCTIONAL MODEL OF A CONDITIONAL ACCESS SYSTEM" EBU REVIEW- TECHNICAL, BE, EUROPEAN BROADCASTING UNION, no. 266, 21 décembre 1995 (1995-12-21), pages 64-77, XP000559450 Grand Saconnex, CH ISSN: 0251-0936 page 67, colonne de droite, ligne 25 -page 76, colonne de droite, ligne 5 figures 4-7	4-6, 9-13
<input type="checkbox"/> Voir la suite du cadre C pour la fin de la liste des documents <input checked="" type="checkbox"/> Les documents de familles de brevets sont indiqués en annexe		
* Catégories spéciales de documents cités:		
"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent "E" document antérieur, mais publié à la date de dépôt international ou après cette date "L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée) "O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens "P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée "T" document ultérieur publié après la date de dépôt international ou la date de priorité et s'appliquant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention "X" document particulièrement pertinent: l'inventeur revendiqué ne peut être considéré comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément "Y" document particulièrement pertinent: l'inventeur revendiqué ne peut être considéré comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier "Z" document qui fait partie de la même famille de brevets		
Date à laquelle la recherche internationale a été effectivement achevée 18 octobre 2001		Date d'expédition du présent rapport de recherche internationale 25/10/2001
Nom et adresse postale de l'administration chargée de la recherche internationale Office Européen des Brevets, P.B. 5618 Palatzaan 2 NL - 2280 HV Rijswijk Tel: (+31-70) 340-2040, Tx: 31 651 epo nl, Fax: (+31-70) 340-3016		Fonctionnaire autorisé Van der Zaal, R

RAPPORT DE RECHERCHE INTERNATIONALE

Der
internationale No
PCT/FR 01/02174

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 9919822	A	22-04-1999	EP 1031206 A2 WO 9919822 A2	30-08-2000 22-04-1999